UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,380	02/14/2002	Howard S. Lambert	GB920010010US1	1350

7590 01/17/2006

IBM Corp, IP Law
11400 Burnett Road, Zip 4054
Austin, TX 78758

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/076,380	LAMBERT, HOWARD S.	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5-10,12-15, 17-25,and 27-38* is/are pending in the application.

4a) Of the above claim(s) *31-38* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5-10,12-15, 17-25, and 27-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Decryption/Encryption Device using Chaotic Encryption."

Response to Amendment

Applicant elected group I, claims 1, 3-10, 12-15, 17-25, 27-30 without traverse in paper filed 10/31/05. Claims 31-38 are withdrawn from further consideration as being drawn to non-elected invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5-10, 12-15, 17, 19-25, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kohda et al (6,014,445) in view of the article by Yu-Huang et al (Dynamic data encryption system based on synchronized chaotic systems).

In reference to claims 1 and 15, Kohda discloses a system for enciphering a real-valued sequence along a chaotic orbit (abstract). The system of Kohda discloses defining starting conditions of the variables of the chaotic equation in the form of an input key (Kohda column 18

lines 35-41), wherein the method includes an iterate step of updating the chaotic equation and the input key for each iteration value and in the decryption of data (column 13 lines 5-10).

However Kohda does not expressly disclose selecting a chaotic equation if a data item is skipped and not received applying the chaotic equation to each data item, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

Yu-Huang discloses a system for a dynamical encryption and decryption system. The system discloses selecting a chaotic equation (Yu-Huang page 272 Fig. 1 and 3rd paragraph); if a data item is skipped and not received (page 272 paragraph 3 column 2), applying the chaotic equation to each data item (page 272 first full paragraph and (Fig. 1), the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result (page 272 paragraph 3 column 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to uses the dynamic data encryption of Yu-Huang in the system of Kohda. One of ordinary skill in the art would have been motivated to do this because the system is more secure in the sense that distinct attractors are used.

In reference to claims 3 and 17, wherein an update chaotic equation is applied to each subsequent data item (Fig. 1).

In reference to claims 5 and 19 wherein the encrypted data item is defned as v = (v xor |z(n+l)|)mod v(max) where z(n+1) is the value of the chaotic equation and vmax is the maximum value of v (Fig. 1).

In reference to claims 6, 20 and 30, where the data is a continuous stream of data items

(Fig. 1).

In reference to claims 7 and 21 wherein the stream of data items has a rate dependency (column 16 lines 60-67).

In reference to claims 8 and 23, wherein the data item is a byte a word or a dword (Fig. 1).

In reference to claims 9 and 24 wherein the chaotic equation is one of a group that can comprise: Fractal equations

Julia sets, Lorenz attractor, Rossler attractor, Hnon attractor, Gumowski/Mira attractor and Tinkerbell attractor (column 13 lines 5-10).

In reference to claims 10 and 25 wherein defined variables of the equation are the key to the encryption and are required at the encrypting source and the decrypting receiver (Fig. 1).

In reference to claims 12 and 27, wherein the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data.

Kohda discloses the use of bit-stream, which is easily converted into block data. However Kohda does not disclose the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data

Yu-Huang discloses a system for a dynamical encryption and decryption system. The system groups the data items in blocks with each block having an identifier providing information of the position of the block in the data (page 272).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to group the data in blocks of data as in Yu-Huang in the system of Kohda. One

of ordinary skill in the art would have been motivated to do this because it would increase the speed of processing.

In reference to claims 13 and 28, wherein the identifier is not encrypted.

Kohda discloses the use of bit-stream, which is easily converted into block data. However Kohda does not disclose the data items are grouped in blocks with each block having an identifier providing information of the position of the block in the data

Yu-Huang discloses a system for a dynamical encryption and decryption system. The system groups the data items in blocks with each block having an identifier providing information of the position of the block in the data (page 272). The identifier of this system is not encrypted.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to group the data in blocks of data as in Yu-Huang in the system of Kohda. One of ordinary skill in the art would have been motivated to do this because it would increase the speed of processing.

In reference to claims 14 and 29, wherein a mask is generated for each block by applying the chaotic equation to each data item in the block (Fig. 1).

In reference to claim 22, wherein the apparatus includes a plurality of defined chaotic equations.

However Kohda does not expressly disclose selecting a chaotic equation if a data item is skipped and not received applying the chaotic equation to each data item, the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result.

Yu-Huang discloses a system for a dynamical encryption and decryption system. The system discloses selecting a chaotic equation (Yu-Huang page 272 Fig. 1 and 3rd paragraph); if a data item is skipped and not received (page 272 paragraph 3 column 2), applying the chaotic equation to each data item (page 272 first full paragraph and (Fig. 1), the method includes applying the iterate step of the chaotic equation for the skipped data item and discarding the result (page 272 paragraph 3 column 2). The system of Yu-Huang discloses a plurality of defined chaotic equations as listed in the Fig. 1.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to uses the dynamic data encryption of Yu-Huang in the system of Kohda. One of ordinary skill in the art would have been motivated to do this because the system is more secure in the sense that distinct attractors are used.

Claims 4 and 18 arerejected under 35 U.S.C. 103(a) as being unpatentable over Kohda in view of Yu-Huang as applied to claims 1 and 15 above, and further in view of Schneier's book (Applied Crytography).

In reference to claims 4 and 18 wherein the step of applying the chaotic equation to the data item includes applying a modular arithmetic operation to combine the real and imaginary parts of the result of the chaotic equation and the data item.

Neither Kohda nor Yu-Huang discloses applying modular arithmetic operations to combine the real and imaginary parts of the result of the chaotic equation and the data item.

Schneier discloses the user of modular arithmetic in cryptographic systems (page 243).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use modular arithmetic as discloses by Schneier in the system of Kohda. One of ordinary skill in the art would have been motivated to do this because modular arithmetic is easier to work with on computers because it restricts the range of all intermediate values and the result (page 243).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Tuesday, December 20, 2005